Birmingham City Council

Standard for Data Encryption

If you have inquiries about this Standard,
Contact the Information and Strategy Team on 0121 675 1431 or 0121 464 2877.

Standard Owner:	***Gerry McMullan – Information and Strategy Manager*** ***Birmingham City Council***
Author:	***Gerry McMullan – Information and Strategy Manager*** ***Birmingham City Council***
Version:	Version 3.0
Date:	04/01/2012
Classification:	Not Protectively Marked

1. OVERVIEW AND PUBLICATION PARTICULARS

Document History

Version Amendment	Date	Purpose	Author
Draft 0.1	31.11.2009	Initial Draft	Gerry McMullan
Version 1.0	09.12.2009	Approved by BTAG	Gerry McMullan
Version 1.2	03.12.2010	Final draft	Gerry McMullan
Version 2.0	08.12.2010	Approved by BTAG	Gerry McMullan
Version 3.0	04.01.2012	Approved by BTCG	Gerry McMullan

Document Distribution after approval

Version	Name	Organisation
1.0	Policies, Standards, Procedures and Guidance Database	Birmingham City Council
2.0	Policies, Standards, Procedures and Guidance Database	Birmingham City Council
3.0	Policies, Standards, Procedures and Guidance Database	Birmingham City Council

Document Reviewers

Version Amendment	Date	Name	Organisation	Role
1.0	Nov 2009	CISG	BCC/Service Birmingham	Reviewer
2.0	Dec 2010	CISG	BCC/Service Birmingham	Reviewer
3.0	Dec 2011	CISG	BCC/Service Birmingham	Reviewer

Document Approval by Birmingham City Council

Version	Date	Name	Role
1.0	09.12.09	BTAG	Approval Body
2.0	08.12.2010	BTAG	Approval Body
3.0	04/01/2012	BTCG	Approval Body

Overview

Authority[a]	Birmingham City Council – Assistant Director Performance and Information	
Owner[b]	Birmingham City Council – Information and Strategy Manager	
Scope[c]	All information held, indexed, classified, processed, stored, transferred, transmitted, used, declassified or disposed of, either by Birmingham City Council, or on behalf of Birmingham City Council by a third party.	
Review period[d]	This document should be reviewed at least annually.	
Related documents	BCC Corporate IS/IT and Information Strategy	
ISO 27001:2005 control references	Control Reference A.10.7.1 Management of removable media A.10.7.3 Information handling procedures A.10.8.1 Information exchange policies and procedures A.10.8.3 Physical media in transit A.10.8.5 Business information systems A.15.1.1 Identification of applicable legislation A.15.1.3 Protection of organisational records A.15.1.5 Prevention of misuse of information processing facilities A.15.1.6 Regulation of cryptographic controls A.15.2.1 Compliance with security policies and standards	

[a] AUTHORITY: The person or organisation who is responsible for enforcing this standard.
[b] OWNER: The organisational position of the person who has rights to authorise changes to, or disposal of this standard
[c] SCOPE: The organisations or persons to whom the standard applies.
[d] REVIEW PERIOD: How frequently the standard should be reviewed.

2. PURPOSE OF THE DATA ENCRYPTION STANDARD

The Birmingham City Council Standard for Data Encryption contains compulsory rules for encrypting data controlled by Birmingham City Council or by Service Birmingham on behalf of Birmingham City Council[e].

Birmingham City Council requires all those within the scope of the standard to follow these rules to protect the confidentiality, integrity and availability of information within the scope of the Standard.

Definition

Data encryption is the process by which information readable by human beings is scrambled by

Scope

The Standard covers all defined data[f] processed either by Birmingham City Council or on behalf of Birmingham City Council by a third party.

Data may be electronic, graphic, microfiche, film, audio-tape, printed, hand-written, spoken, displayed or stored on any medium.

The obligations outlined in this standard apply as required to employees, agency staff, elected members (or other public representatives), trustees, third parties under a contract, employees of associated organisations or volunteers. It applies as appropriate to those who work at home or from home or have remote or flexible patterns of working.

This standard is part of the Birmingham City Council Information Security Policy Framework and it should be brought to the attention of all within the scope of this Standard when their relationship with Birmingham City Council or Service Birmingham begins, materially changes and ends, at regular intervals[g].

[e] In line with ISO 27001:2005 A.7:2:2

[f] Data is processed whenever information is indexed, classified, stored, recorded, disseminated, published, copied, organised, amended, retrieved, viewed, disclosed to others, deleted, destroyed, transferred, transmitted, declassified: *it is difficult to say there is any activity directed towards the data, which does not amount to processing.*

[g] It should be incorporated into certain contracts; employment induction packs; rules for elected members and volunteers, conditions of use of Birmingham City Council facilities, leaving procedures &c..

3. STANDARD PARTICULARS

Background information

All data held on Birmingham City Council computers or being transmitted or carried between systems or across networks needs to be protected against accidental or deliberate loss or destruction. Data encryption provides one of the key services needed to provide the City Council with the assurance that the necessary protections are in place for data which is moved between systems or is being transported in a form which makes it vulnerable.

Specific policy or technical requirements to encrypt Council data or data provided by partner organisations may be imposed by legislation or under agreements with those partners or competent public authorities. These include complying with the provisions of the Data Protection Act 1998 and the obligations accepted by the City Council in Memoranda of Understanding (MoUs) signed with particular Central Government departments.

Core requirements

All desktop and laptop machines provided by the City Council for work purposes will include data encryption as an integral part of the standard machine image. The active use of data encryption will form one of the standard services run on City Council machines.

Where authorisation has been given for the use of personal machines to process City Council data, this authorisation may include the requirement to use data encryption. The City Council may, at its discretion, provide standalone encryption software to be installed on personal machines.

The deployment and operation of data encryption services will be controlled corporately and managed wherever possible by means of a single configuration covering all devices. Corporate control will provide the safeguard of being able to recover in a secure and fully audited way any data where the owner has lost or forgotten the password and needs to decrypt it.

The use of standalone encryption on City Council supplied or supported machines will normally only be agreed if:

- there is an insuperable technical problem in deploying centrally managed encryption and a security assessment has determined that there are no major risks with deploying standalone encryption; or
- a specific standalone solution is required by an external partner or supplier and a security assessment has determined that there are no major risks with deploying this solution

Corporate responsibility for setting and reassessing the policy for the use of data encryption will lie with the Information and Strategy team in Corporate Resources.

Responsibility with managing the corporate data encryption service will lie with the Service Birmingham Service Desk.

Individual users will not normally be required to manage or configure the encryption of data installed on machines. They will however be required to set and maintain (including protecting form theft, loss or accidental disclosure) passwords for any files copied to removable media.

This standard will not apply automatically to the encryption of files sent as attachments to e-mail messages. Separate advice on the security of e-mail messages is contained in the

Messaging Code of Practice

Detailed procedures for managing the data encryption services will be developed as required. Any procedures will be subject to approval by the Business Transformation Coordination Group and once approved will be published on the PSPG database.

Elements of the Standard

The minimal acceptable level of encryption on the standard image will be 128-bit encryption.

Higher levels of encryption may be defined as mandatory in order to comply with specific requirements – such as the use of the FIPS 140-2 standard for certain government applications or to meet the requirements of higher levels of Protective Marking than the City Council would normally be expected to apply: i.e. Protective Marking higher than RESTRICTED.

Data encryption will be applied to all removable media other than those given a specific exemption for technical or policy reasons by the Information and Strategy Team in Corporate Resources. A password will be generated for all data copied to a removable medium. Passwords for encrypted files should conform to the rules laid out in the Password Control Standard.

4. ROLES AND RESPONSIBILITIES

Role	Organisation	Responsibility
All within scope of this Standard (see above)	All within Scope	to follow this Standard and any associated Codes of Practice or procedures
Corporate Management Team	Birmingham City Council	for the management of the City Council's information assets; to manage and maintain controls which limit access to information as required in this Standard; to assess information provided by local managers.
Performance and Information division Information and Strategy Manager	Birmingham City Council	to manage the Data Encryption Standard to meet the Council's requirements and to make sure it is reviewed at least annually; to maintain the register of approved schemas.
Birmingham City Council Managers	Birmingham City Council; Service Birmingham on behalf of Birmingham City Council.	to ensure compliance with the Standard in all relevant City Council systems; to communicate this Standard and any associated Code to staff and others within the scope (see above); to make sure third party organisations are aware of the City's Council's Standard for Encryption; to liaise with the Business Policy Team on any issues which may affect the management of the encryption service to communicate issues and anomalies back to the Business Policy Team.

5. EXCEPTIONS

There are no exceptions to this Standard.

6. ENFORCEMENT

Any individual member of staff who contravenes this Standard may be investigated under the Council's disciplinary procedure and, where appropriate, legal action may be taken.

Other individuals within the scope of this Standard may be investigated and, where appropriate, legal action may be taken against them, or withdrawal of privileges. Third parties or partner organisations who contravene this Standard may jeopardise their relationship with Birmingham City Council and may also face legal action.